Proving Resistance against Invariant Attacks: Properties of the Linear Layer (Extended Abstract)

Christof Beierle[1], Anne Canteaut[2], Gregor Leander[1], and Yann Rotella[2]

[1] Horst Görtz Institute for IT Security, Ruhr-Universität Bochum, Germany
christof.beierle@rub.de, gregor.leander@rub.de
[2] Inria, Paris, France
anne.canteaut@inria.fr, yann.rotella@inria.fr

Abstract. Many lightweight block ciphers use a very simple key-schedule where the round-keys only differ by a round-constant. However, several of those schemes were recently broken using invariant attacks, i.e. invariant subspace attacks or nonlinear invariant attacks. This work analyzes the resistance of such ciphers against invariant attacks and reveals the precise mathematical properties that render those attacks applicable. As a first practical consequence, we prove that some ciphers including Prince, Skinny-64 and Mantis_7 are not vulnerable to invariant attacks. Also, we show that the invariant factors of the linear layer have a major impact on these attacks. Most notably, if the number of invariant factors of the linear layer is small (e.g., if its minimal polynomial has a high degree), we can easily find round-constants which guarantee the resistance to all types of invariant attacks, independently of the choice of the Sbox-layer.

One of the main topics in symmetric cryptography in recent years is lightweight cryptography. Even though it is not really clearly defined what lightweight cryptography exactly is, the main idea can be embraced as designing cryptographic primitives that put an extreme focus on performance. This in turn resulted in many new, especially block cipher, designs which achieve better performance by essentially removing any operations that are not strictly necessary (or believed to be necessary) for the security of the scheme. One particular interesting case of reducing the complexity is the design of the key schedule and the choice of round constants. Both of these are arguably the parts that we understand least and only very basic design criteria are available on how to choose a good key schedule or how to choose good round constants. Consequently, many of the lightweight block ciphers remove the key schedule completely. Instead, identical keys are used in the rounds and (often very simple and sparse) round constants are added on top (e.g., see LED [5], Skinny [1], Prince [2], Mantis [1], to mention a few).

However, several of those schemes were recently broken using a structural attack called invariant subspace attack [7, 8], as well as the recently published generalization called nonlinear invariant attack [10]. Indeed, those attacks have been successfully applied to quite a number of recent designs including PRINTcipher [7], Midori64 [4, 10], iSCREAM [8] and SCREAM [10], NORX v2.0 [3], Simpira v1 [9] and Haraka v.0 [6]. Both attacks, that we jointly call *invariant attacks* in this work, notably exploit the fact that these lightweight primitives have a very simple key schedule where the same round key (up to the addition of a round constant) is applied in several rounds.

It is therefore of major importance to determine whether a given primitive is vulnerable to invariant attacks. More generally, it would be interesting to exhibit

some design criteria for the building blocks in a cipher which guarantee the resistance against these attacks. As mentioned above, this would shed light on the fundamental open question on how to select proper round constants.

In this work, we analyze the resistance of several lightweight substitution-permutation ciphers against invariant attacks. Our framework both covers the invariant subspace attack, as well as the recently published nonlinear invariant attack. By exactly formalizing the requirements of those attacks, we are able to reveal the precise mathematical properties that render those attacks applicable. Indeed, as we will detail below, the rational canonical form of the linear layer will play a major role in our analysis. Our results show that the linear layer and the round constants have a major impact on the resistance against invariant attacks, while this type of attacks was previously believed to be mainly related to the behaviour of the S-box, see e.g. [4]. In particular, if the number of invariant factors of the linear layer is small (for instance, if its minimal polynomial has a high degree), we can easily find round constants which guarantee the resistance to all types of invariant attacks, independently of the choice of the S-box layer.

In our framework, the resistance against invariant attacks is defined in the following sense: For each instantiation of the cipher with a fixed key, there is no function that is invariant for both the substitution layer and for the linear part of each round. This implies that any adversary who still wants to apply an invariant attack necessarily has to search for invariants over the *whole round function*, which appears to have a cost exponential in the block size in general. Indeed, all published invariant attacks we are aware of exploit weaknesses in the underlying building blocks of the round. Therefore, our notion of resistance guarantees complete security against the major class of invariant attacks, including all variants published so far.

This work is split in two parts, a first part which can be seen as the attacker's view on the problem and a second part which reflects more on the designer's decision on how to avoid those attacks. More precisely, the first part details an algorithmic approach which enables an adversary to spot a possible weakness with respect to invariant attacks within a given cipher. For the lightweight block ciphers Skinny-64, Prince, and Mantis$_7$, this algorithm is used to prove the resistance against invariant attacks.

These results come from the following observation, detailed in this first part: Let L denote the linear layer of the cipher in question and let $c_1, \ldots, c_t \in \mathbb{F}_2^n$ be the (XOR) differences between two round constants involved in rounds where the same round key is applied. Furthermore let $W_L(c_1, \ldots, c_t)$ denote the smallest L-invariant subspace of $\mathbb{F}_2^n$ that contains all $c_1, \ldots, c_t$. Then, one can guarantee resistance if $W_L(c_1, \ldots, c_t)$ covers the whole input space $\mathbb{F}_2^n$. As a direct result, we will see that in Skinny-64, there are enough differences between round constants to guarantee the full dimension of the corresponding L-invariant subspace. This directly implies the resistance of Skinny-64, and this result holds *for any choice of the S-box layer*.[1] In contrast, for Prince and Mantis$_7$, there are not enough suitable c_i to generate a subspace $W_L(c_1, \ldots, c_t)$ with full dimension. However, for both primitives, we are able to keep the security argument by also considering the S-box layer, using the fact that the dimension of $W_L(c_1, \ldots, c_t)$ is not too low in both cases.

In the second part, we provide an in-depth analysis of the impact of the round constants and of the linear layer on the resistance against invariant attacks. The first question we ask is the following:

Given the linear layer L of a cipher, what is the minimum number of round constants needed to guarantee resistance against the invariant attack, independently

[1] We have to provide that the S-box has no component of degree 1. However, if the S-box has such a linear component, the cipher could be easily broken using linear cryptanalysis.

from the choice of the S-box?

Figure 1 shows the maximal dimension that can be reached by $W_L(c_1, \ldots, c_t)$ when t values of c_i are considered.

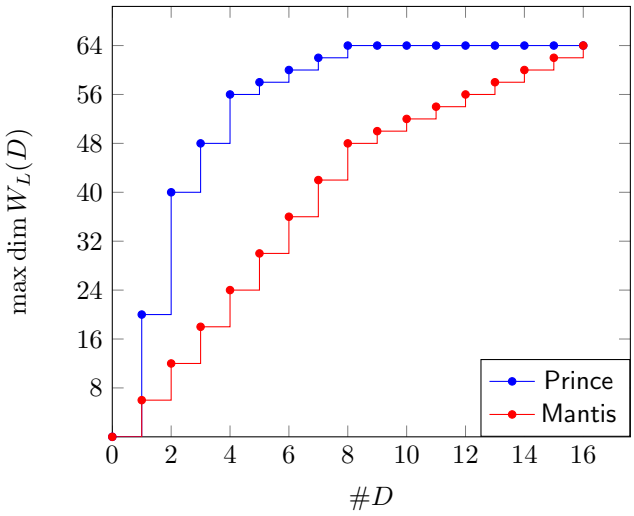

Fig. 1. For the linear layer of Skinny-64, Prince and Mantis, this figure shows the highest possible dimension of $W_L(c_1, \ldots, c_t)$ for t values $c_1, \ldots, c_t$ (see Theorem 1).

It shows in particular that the whole input space can be covered with only $t = 4$ values in the case of Skinny-64, while 8 and 16 values are needed for Prince and Mantis respectively. This explains why, even though Prince and Mantis apply very dense round constants, the dimension does not increase rapidly for higher values of t.

The observations in Fig. 1 are deduced from the *invariant factors* (or the *rational canonical form*) of the linear layer, as shown in the following theorem.

Theorem 1. *Let $Q_1, \ldots, Q_r$ be the invariant factors of the linear layer L and let $t \leq r$. Then*

$$\max_{c_1,\ldots,c_t \in \mathbb{F}_2^n} \dim W_L(c_1, \ldots, c_t) = \sum_{i=1}^{t} \deg Q_i.$$

For the special case of a single constant c, the maximal dimension of $W_L(c)$ is equal to the degree of the greatest invariant factor of L, i.e. the minimal polynomial of L. We will also explain how the particular round constants must be chosen in order to guarantee the best possible resistance.

As designers often choose random round constants to instantiate the primitive, we were also interested in the following question:

How many randomly chosen round constants are needed to guarantee the best possible resistance with a high probability?

We derive an exact formula for the probability that the subspace $W_L(c_1, \ldots, c_t)$ has full dimension for t uniformly random constants c_i. Fig. 2 gives an overview of this probability for several lightweight designs.

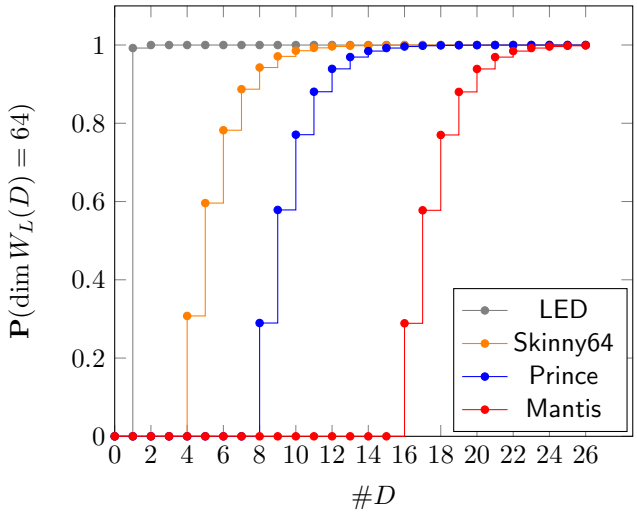

Fig. 2. For the linear layer of several lightweight ciphers, this figure shows the probability that $W_L(c_1, \ldots, c_t) = \mathbb{F}_2^n$ for uniformly random chosen constants c_i.

References

1. Beierle, C., Jean, J., Kölbl, S., Leander, G., Moradi, A., Peyrin, T., Sasaki, Y., Sasdrich, P., Sim, S.M.: The SKINNY family of block ciphers and its low-latency variant MANTIS. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016, Part II. LNCS, vol. 9815, pp. 123–153. Springer (2016)
2. Borghoff, J., Canteaut, A., Güneysu, T., Kavun, E.B., Knežević, M., Knudsen, L.R., Leander, G., Nikov, V., Paar, C., Rechberger, C., Rombouts, P., Thomsen, S.S., Yalçin, T.: PRINCE - A low-latency block cipher for pervasive computing applications - extended abstract. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 208–225. Springer (2012)
3. Chaigneau, C., Fuhr, T., Gilbert, H., Jean, J., Reinhard, J.R.: Cryptanalysis of NORX v2.0. IACR Trans. Symmetric Cryptol. 2017(1) (2017), to appear
4. Guo, J., Jean, J., Nikolic, I., Qiao, K., Sasaki, Y., Sim, S.M.: Invariant Subspace Attack Against Midori64 and The Resistance Criteria for S-box Designs. IACR Trans. Symmetric Cryptol. 2016(1), 33–56 (2016)
5. Guo, J., Peyrin, T., Poschmann, A., Robshaw, M.J.B.: The LED block cipher. In: Preneel, B., Takagi, T. (eds.) CHES 2011. LNCS, vol. 6917, pp. 326–341. Springer (2011)
6. Jean, J.: Cryptanalysis of Haraka. IACR Trans. Symmetric Cryptol. 2016(1), 1–12 (2016)
7. Leander, G., Abdelraheem, M.A., AlKhzaimi, H., Zenner, E.: A cryptanalysis of PRINTcipher: The invariant subspace attack. In: Rogaway, P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 206–221. Springer (2011)
8. Leander, G., Minaud, B., Rønjom, S.: A generic approach to invariant subspace attacks: Cryptanalysis of Robin, iSCREAM and Zorro. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015, Part I. LNCS, vol. 9056, pp. 254–283. Springer (2015)
9. Rønjom, S.: Invariant subspaces in Simpira. Cryptology ePrint Archive, Report 2016/248 (2016), `http://eprint.iacr.org/2016/248`
10. Todo, Y., Leander, G., Sasaki, Y.: Nonlinear invariant attack - practical attack on full SCREAM, iSCREAM, and Midori64. In: Cheon, J.H., Takagi, T. (eds.) ASIACRYPT 2016, Part II. LNCS, vol. 10032, pp. 3–33. Springer (2016)